PURPOSE

The purpose is to establish the policy and procedure for the Michigan Department of Health and Human Services (MDHHS) to ensure that workforce members have appropriate access to sensitive information and Electronic Protected Health Information (ePHI) and to prevent those who do not have access from accessing protected and confidential information. Termination Procedures are to halt access to sensitive information and ePHI when the employment of a workforce member or business associate is transferred to another department, when employment ends or for cause.

DEFINITIONS

Availability means that data or information is accessible and useable upon demand by an authorized person.

Confidentiality means that confidential information is not made available or disclosed to unauthorized persons or processes.

ePHI is the acronym for Electronic Protected Health Information. It is Protected Health Information that is transmitted or maintained in electronic form.

PHI is the acronym for Protected Health Information. It is information that can identify a person and contains health related data pertaining to that person.

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications and people.

Integrity means that confidential information has not been altered or destroyed in an unauthorized manner.

Workforce member means employees, volunteers and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, students, volunteers and staff from third party entities who provide service to the covered entity.

POLICY

It is the policy of the MDHHS to prevent the possibility of unauthorized access to secure data by members of the workforce who are no longer authorized to access data will be prevented by taking the following security measures, where applicable, for workforce members that are terminating or changing positions and for business associate relationships that are being terminated.

PROCEDURE

Supervisor/Manager Responsibility

Complete the DCH 1189E, Exiting Employee Check-out List, and any associated forms in relationship to HIPAA security (such as a DCH-0432E, Computer Network Access Request), and submit to human resources. A copy must also be submitted to the HIPAA security officer.

Collect physical access control items (for example, ID badges, smart cards and tokens) that allow access to physical spaces or MDHHS information and any MDHHS issued equipment (for example, cellular phones, portable computer devices, diskettes and other electronic storage media). If possible, this should be accomplished prior to actual departure or position change.

Notify the MDHHS security officer, human resources and other designated areas in order to:

- Block access privileges immediately if needed.
- Deactivate user accounts upon separation unless otherwise communicated by authorized personnel.
- Cancel or re-assign any existing e-mail account(s) and change password(s).
- Notify DTMB to determine if there are any access storage media issues used by the departing workforce member.
- Ensure that any locked files cannot be opened.
- Unsubscribe workforce member from any mailing lists.

DTMB/System Administrators Responsibility

- Affected workforce members or business associates shall be removed from relevant access control lists in a timely manner.
- Affected workforce members shall be deactivated from relevant user accounts in a timely manner.

Supervisors/Maintenance Responsibility

Change combinations on lock mechanisms after departure of workforce member in a timely manner.

REFERENCES

45 CFR 164.308(a)(3)

CONTACT

For additional information concerning this policy and procedure, contact the MDHHS security officer at MDHHSPrivacySecurity@michigan.gov.

DTMB Client Service Center may be contacted at 517-241-9700 or 800-968-2644.